



Operating System

Setting Up Certification Authority Trust for a Domain

Beta 3 Technical Walkthrough

Abstract

This technical walkthrough guides you through the steps to configure a Microsoft Windows® 2000–based domain to trust external certification authorities, using the Group Policy Microsoft Management Console (MMC) snap-in. The Group Policy MMC snap-in allows the administrator to define the external certification authorities that the domain will trust.

© 1999 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, the BackOffice logo, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0499

CONTENTS

INTRODUCTION 1

Prerequisites 1

CREATING A NEW GPO AND ADDING A ROOT CERTIFICATE .. 2

VIEWING THE CERTIFICATE STORE..... 8

FOR MORE INFORMATION 12

Before You Call for Support 12

Reporting Problems 12

INTRODUCTION

This technical walkthrough guides you through the steps to configure a Microsoft Windows® 2000–based domain to trust external certification authorities, using the Group Policy Microsoft Management Console (MMC) snap-in.

The Group Policy MMC snap-in allows the administrator to define the external certification authorities that the domain will trust.

Prerequisites

This technical walkthrough assumes the following environment:

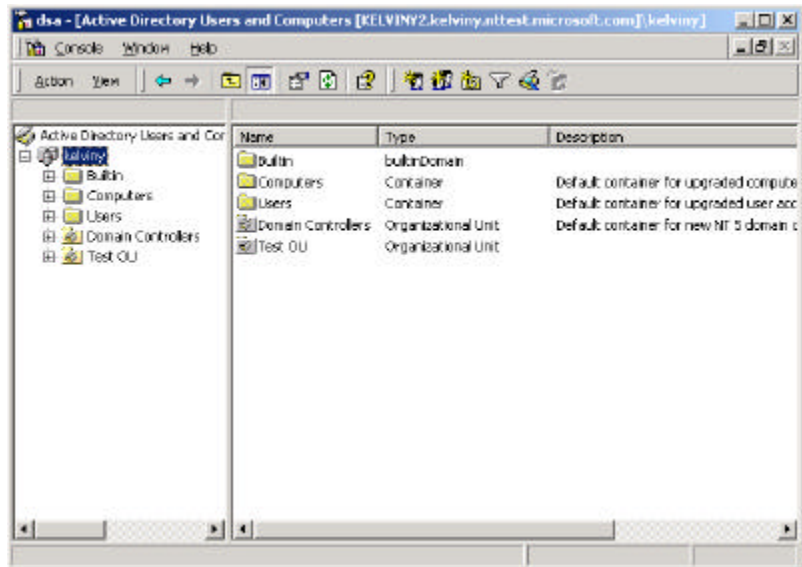
- You have installed Windows 2000 build 1943 and later clients connected to a Windows 2000 domain.
- You are a domain administrator.

CREATING A NEW GPO AND ADDING A ROOT CERTIFICATE

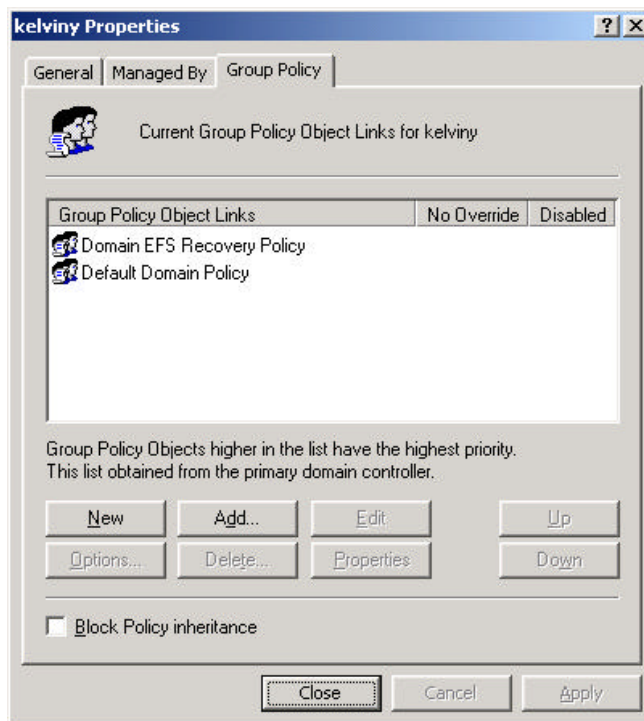
The following steps walk you through adding a new Group Policy Object (GPO), and then adding a root certificate to that GPO.

To create an automatic certificate request in the default GPO

1. Start the Microsoft Active Directory™ directory service Users and Computers snap-in.



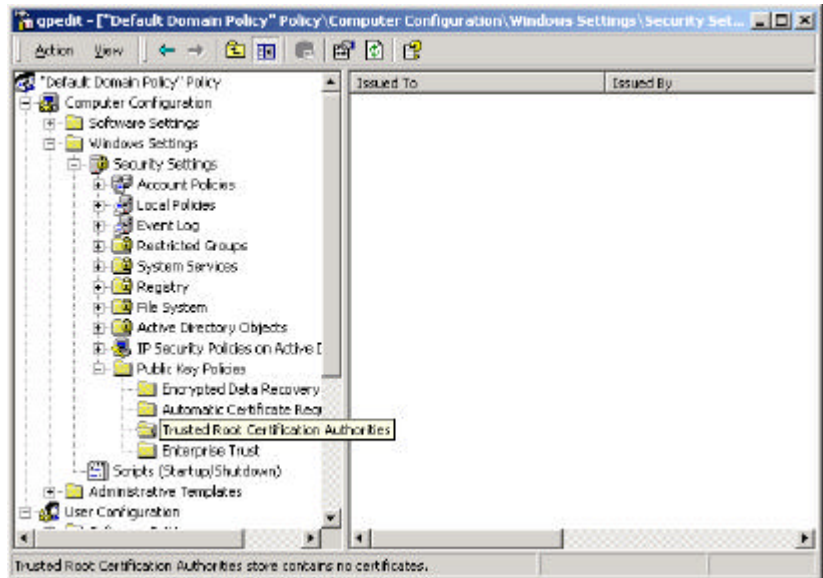
2. Right click the domain node, and select **Properties** to start the Properties dialog box.



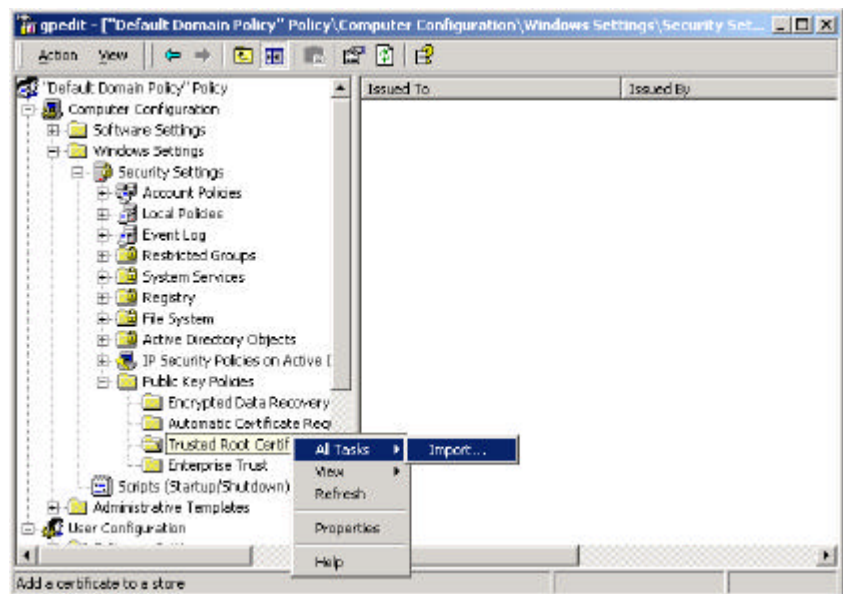
3. By default, Windows creates two GPOs for the domain. Select the **Default**

Domain Policy GPO, and click **Edit**. This starts the Group Policy snap-in.

4. Expand the node hierarchy and navigate to the **Trusted Root Certification Authorities** folder under the **Computer Configuration** node.



5. Right-click the **Trusted Root Certificate Authorities** folder.

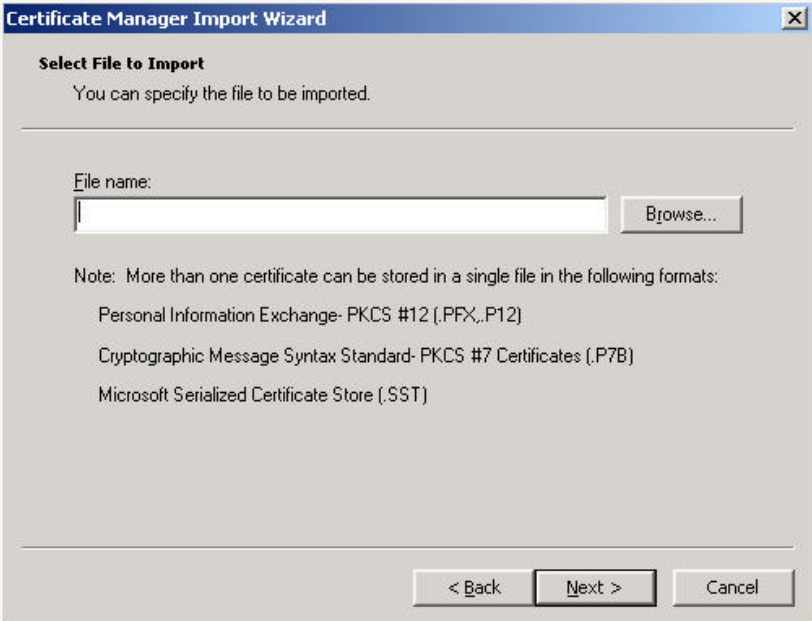


6. On the **All Tasks** submenu, select **Import**. The Certificate Manager Import Wizard starts.



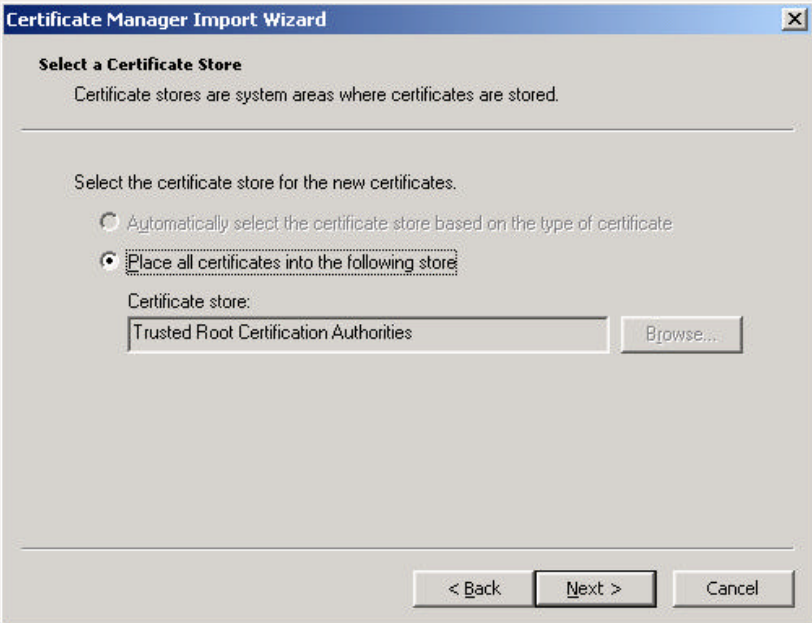
7. Click **Next**.

8. Enter the name of the file that contains the root certificate you want to import.



The screenshot shows the 'Certificate Manager Import Wizard' window, specifically the 'Select File to Import' step. The window has a title bar with the text 'Certificate Manager Import Wizard' and a close button. Below the title bar, the text 'Select File to Import' is displayed, followed by the instruction 'You can specify the file to be imported.' A text box labeled 'File name:' is present, with a 'Browse...' button to its right. Below this, a 'Note' states: 'More than one certificate can be stored in a single file in the following formats:'. Three bullet points follow: 'Personal Information Exchange- PKCS #12 (.PFX,.P12)', 'Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)', and 'Microsoft Serialized Certificate Store (.SST)'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

9. Click **Next**. The destination is the **Trust Root Certificate Authorities** store in the GPO.



The screenshot shows the 'Certificate Manager Import Wizard' window, specifically the 'Select a Certificate Store' step. The window has a title bar with the text 'Certificate Manager Import Wizard' and a close button. Below the title bar, the text 'Select a Certificate Store' is displayed, followed by the instruction 'Certificate stores are system areas where certificates are stored.' Below this, the text 'Select the certificate store for the new certificates.' is shown. There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is unselected) and 'Place all certificates into the following store' (which is selected). Below the selected option, there is a text box labeled 'Certificate store:' containing the text 'Trusted Root Certification Authorities', with a 'Browse...' button to its right. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

10. Click **Finish** to import the certificate.

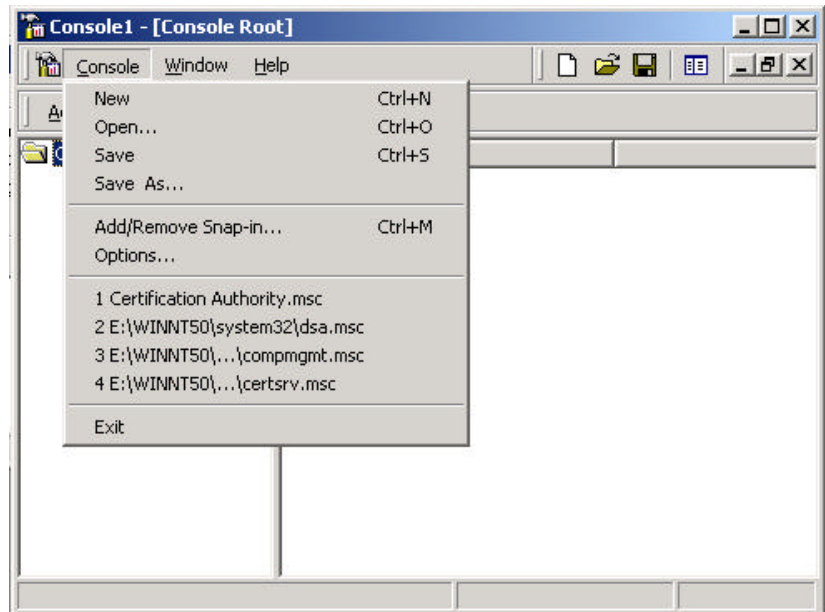


VIEWING THE CERTIFICATE STORE

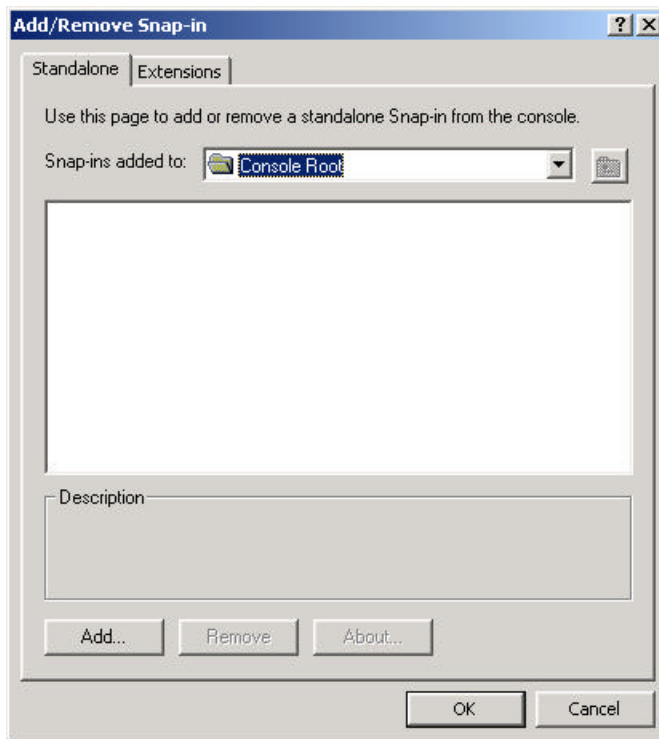
To verify that the root certificate has been imported, you can use the Certificates snap-in to view the computer's certificate store and to verify trust relationships.

To view the certificate store

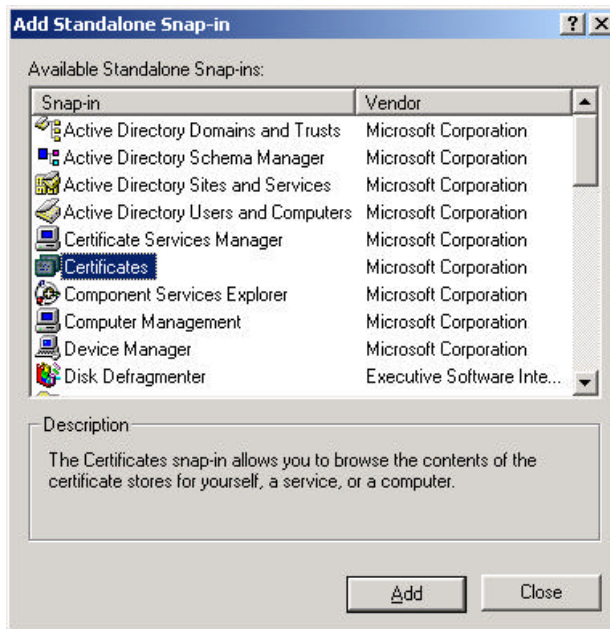
1. Start the Microsoft Management Console. On the **Start** menu, click **Run**. Type `mmc.exe` and click **OK**.



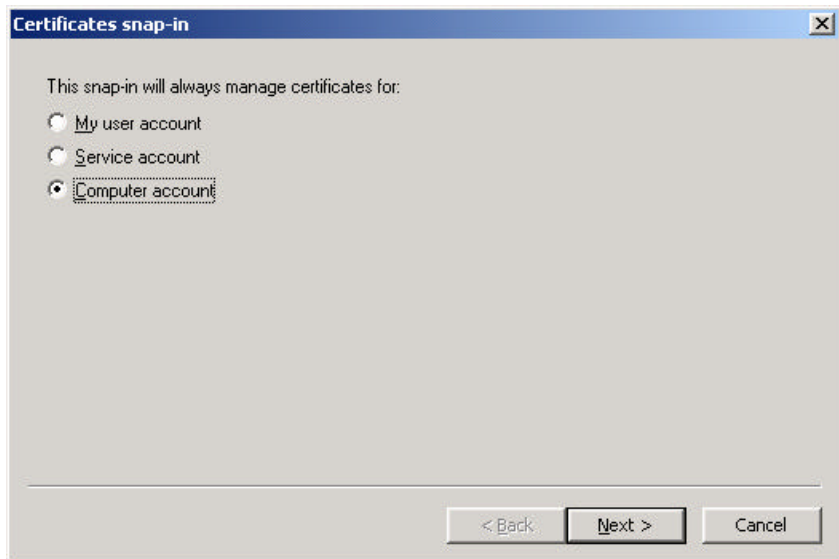
2. On the **Console** menu, select **Add/Remove Snap-in**.



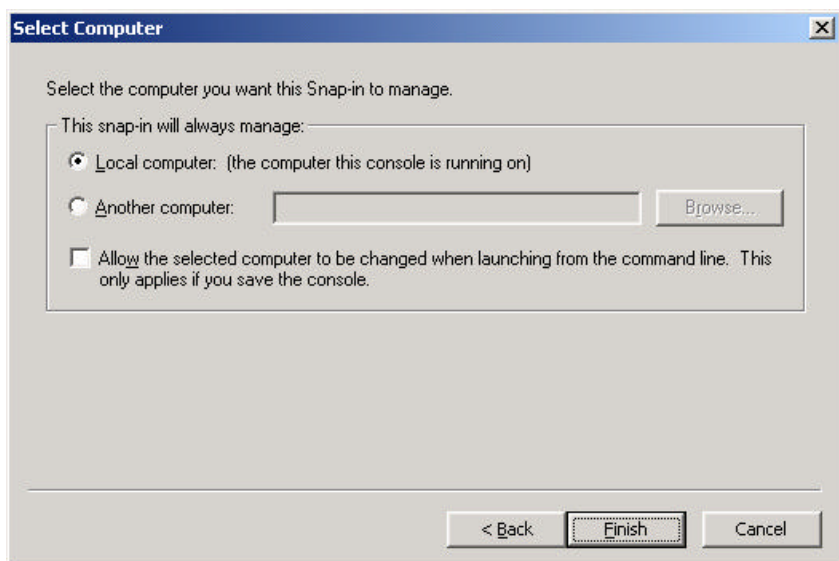
3. Click **Add** to select a snap-in.



4. Select **Certificates** to add the Certificates snap-in.

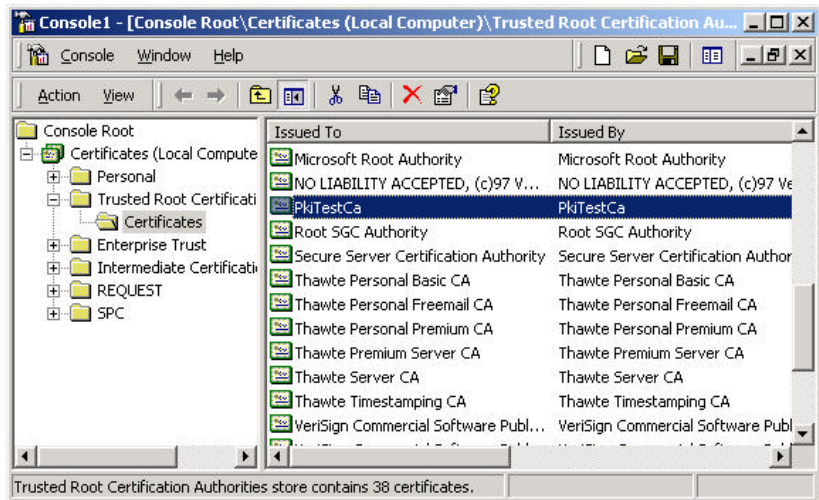


5. Click **Computer account** to manage certificates for a computer. Click **Next** to continue.

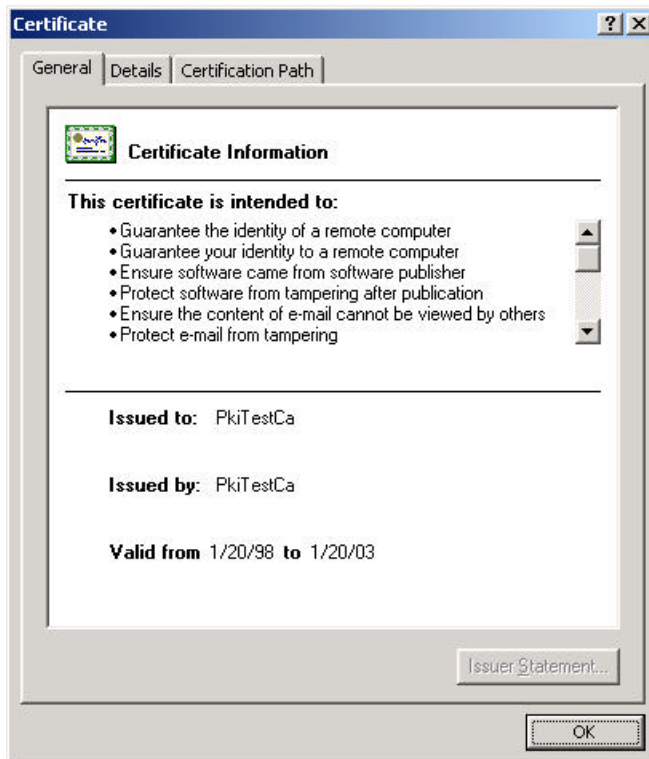


6. Select **Another Computer** and type in the name of the computer. Click **Finish** to continue.

7. Expand the hierarchy under the **Certificates** node in the left pane. Click the **Certificates** folder under the **Trusted Root Certification Authority** folder.



8. Double-click to view a certificate.



FOR MORE INFORMATION

For the latest information on Microsoft Windows 2000 network operating system, visit our World Wide Web site at <http://www.microsoft.com/windows/server/> and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows 2000 Beta 3, visit the World Wide Web site at <http://ntbeta.microsoft.com/>.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported by way of the appropriate bug reporting channel and alias. Please make sure to describe the problem adequately so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.